AMENDMENTS TO THE CLAIMS

LISTING OF CLAIMS

Claim 1 (previously presented): A method for operating a computer system comprising a plurality of computers connected by a network, said computer system including an administrative computer, A, and a client computer, C, said method comprising the steps of:

providing a badge secured to one of said authorized individuals, said badge having a data processing system having a non-volatile memory, a volatile memory, a transceiver for sending and receiving signals utilized by said badge, and an attachment sensor for detecting the removal of said badge from that individual, said attachment sensor causing information stored in said volatile memory to be rendered unreadable when said attachment sensor detects said removal;

providing A with a transceiver for communicating with one of said badges and an identity verification system for authenticating the identity of that individual; and

a1

causing A to load information in said volatile memory of said badge attached to that individual in response to said identity verification system authenticating that individual, said information specifying the level of access to said computer system to which that authorized individual is entitled.

Claim 2 (previously presented): The method of Claim 1 wherein said step of causing A to load information comprises the steps of:

establishing a secure communication channel between A and that badge by encrypting signals sent and received by said transceivers in A and that badge; and

sending said information on said secure communication channel.

Claim 3 (previously presented): The method of Claim 1 wherein said identity verification system compares the retina of that individual with data derived from a previous measurement on that individual's retina.

Claim 4 (previously presented): The method of Claim 1 wherein said identity verification system compares a finger print of that individual with data derived from a previous measurement on that individual's finger print.

Claim 5 (previously presented): The method of Claim 1 wherein said identity verification system compares the voice of that individual with data derived from a previous measurement on that individual's voice.

Claim 6 (previously presented): The method of Claim 1 wherein said identity verification system compares answers to queries posted to that individual with data previously provided by that individual.

Claim 7 (previously presented): The method of Claim 1 further comprising the steps of:

providing C with a transceiver for communicating with said badge attached to that individual;

causing C to verify the authenticity of that badge by receiving data derived from the data stored in said volatile memory of that badge by A;

causing C to provide that individual with access to said network, said access depending on said data stored in said badge.

Claim 8 (previously presented): The method of Claim 7 wherein C periodically verifies the presence of that individual by sending to and receiving signals from that badge.

Claim 9 (previously presented): The method of Claim 8 wherein C utilizes a first secure code to exchange data with that badge during said verification step.

Claim 10 (previously presented): The method of Claim 9 wherein C utilizes a second secure code to verify the presence of that individual, said second secure code requiring less computational resources than said first secure code.

Claim 11 (previously presented): The method of Claim 10 wherein said second secure code depends on said first secure code and changes each time C verifies the presence of that individual.

Claim 12 (previously presented): The method of Claim 1 wherein said information loaded by A into that badge includes a code that is periodically changed.

Claim 13 (new): A method for operating a computer security system comprising:

providing a badge having a data processing system comprising:

a non-volatile memory;

a volatile memory;

a transceiver for sending and receiving signals utilized by said badge; and

a1

an attachment sensor for detecting the removal of said badge from an individual, said attachment sensor causing information stored in said volatile memory to be rendered unreadable when said attachment sensor detects said removal;

providing an identity verification system for authenticating identity of the individual; and

causing an administrative device to load information in said volatile memory of said badge in response to said identity verification system authenticating the individual, said information specifying the level of access to said computer system to which the individual is entitled.

Claim 14 (new): The method of Claim 13 wherein said causing the administrative device to load information comprises:

establishing a secure communication channel between the administrative device and that badge by encrypting signals sent and received by said transceivers in the administrative device and that badge; and sending said information on said secure communication channel.

Claim 15 (new): The method of Claim 13 wherein said identity verification system compares the retina of the individual with data derived from a previous measurement on the individual's retina.

Claim 16 (new): The method of Claim 13 wherein said information loaded by the administrative device into the badge includes a code that is periodically changed.

Claim 17 (new): A security badge comprising:

a non-volatile memory;

a volatile memory;

a transceiver for sending and receiving signals utilized by said badge; and

a\

an attachment sensor for detecting the removal of said badge from an individual, said attachment sensor causing information stored in said volatile memory to be rendered unreadable when said attachment sensor detects said removal;

wherein an administrative device may load information in said volatile memory of said badge in response to an identity verification system authenticating an individual maintaining said badge, said information specifying the level of access to a computer system to which the individual is entitled.

Claim 18 (new): The method of Claim 17 wherein said information loaded by the administrative device into the badge includes a code that is periodically changed.

Claim 19 (new): The method of Claim 17 wherein the administrative device loading information comprises:

establishing a secure communication channel between the administrative device and that badge by encrypting signals sent and received by said transceiver in the badge; and

sending said information on said secure communication channel.